November 1994/Number 3-94

security awareness bulletin

Inside:

Acquisition Systems Protection II

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Security Education and Awareness Team, 8000 Jefferson Davis Hwy, Bldg 33E, Richmond VA 23297-5091; (804) 279-5314, DSN 695-5314. Fax: (804) 279-5239 or DSN 695-5239. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods .

New distribution, address changes:

Government agencies: DoD Security Institute, 8000 Jefferson Davis Hwy, Richmond VA 23297-5091, POC Del Carrell, (804) 279-5314, DSN 695-5314; fax (804) 279-6406, DSN 695-6406

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria VA 22314-1651

DISP contractors: Automatic distribution to each cleared facility. Send change of address to your DIS field office.

Acquisition Systems Protection...*revisited*

The April 1993 issue of the Bulletin introduced the Acquisition Systems Protection Program to our readership. This month's issue is the second installment on our coverage of this new and challenging program. We have made an effort this time to include information that should assist security professionals and program managers in the task of development of their Program Protection Plan. As discussed in the earlier issue, a PPP is to be established for each program to identify and protect classified and other sensitive information from hostile intelligence collection or unauthorized disclosure. The Acquisition Systems Protection Program itself provides a threat-based approach to risk management and tailoring of security countermeasures, and is being used to reduce costs and establish focused protection priorities.

For our lead article we turn again to Edward P. Casey, a recognized authority on the ASPP who has been heavily involved in program protection planning in the military services and defense agencies. Mr. Casey brings us up to date on the June 1994 Joint Security Commission Report and its impact on the ASPP and its stress on risk management. His article includes summaries of DOD, Army, Navy, and Air Force perspectives and implementation activities. This is followed by a short piece by U.S. Army Major Robert Newton that summarizes the process of developing a protection plan, beginning with the identification of the EPITS.

As there have been concerns voiced about how to obtain intelligence threat information, I interviewed Ms. Ruth Ann Jones, Acquisition Security Program Manager for the National Aero-Space Plane Joint Program and Wright-Patterson Air Force Base. The text of her responses are included in this issue along with her process flow chart which she uses in formal presentations about the program. Lastly, we all know that there will still be unanswered questions, particularly from those developing a Program Protections Plan for the first time. Doug Cavileer at OSD has provided us with a list of points of contact in key organizations who stand ready to field questions.

Lynn Fischer, Senior Editor

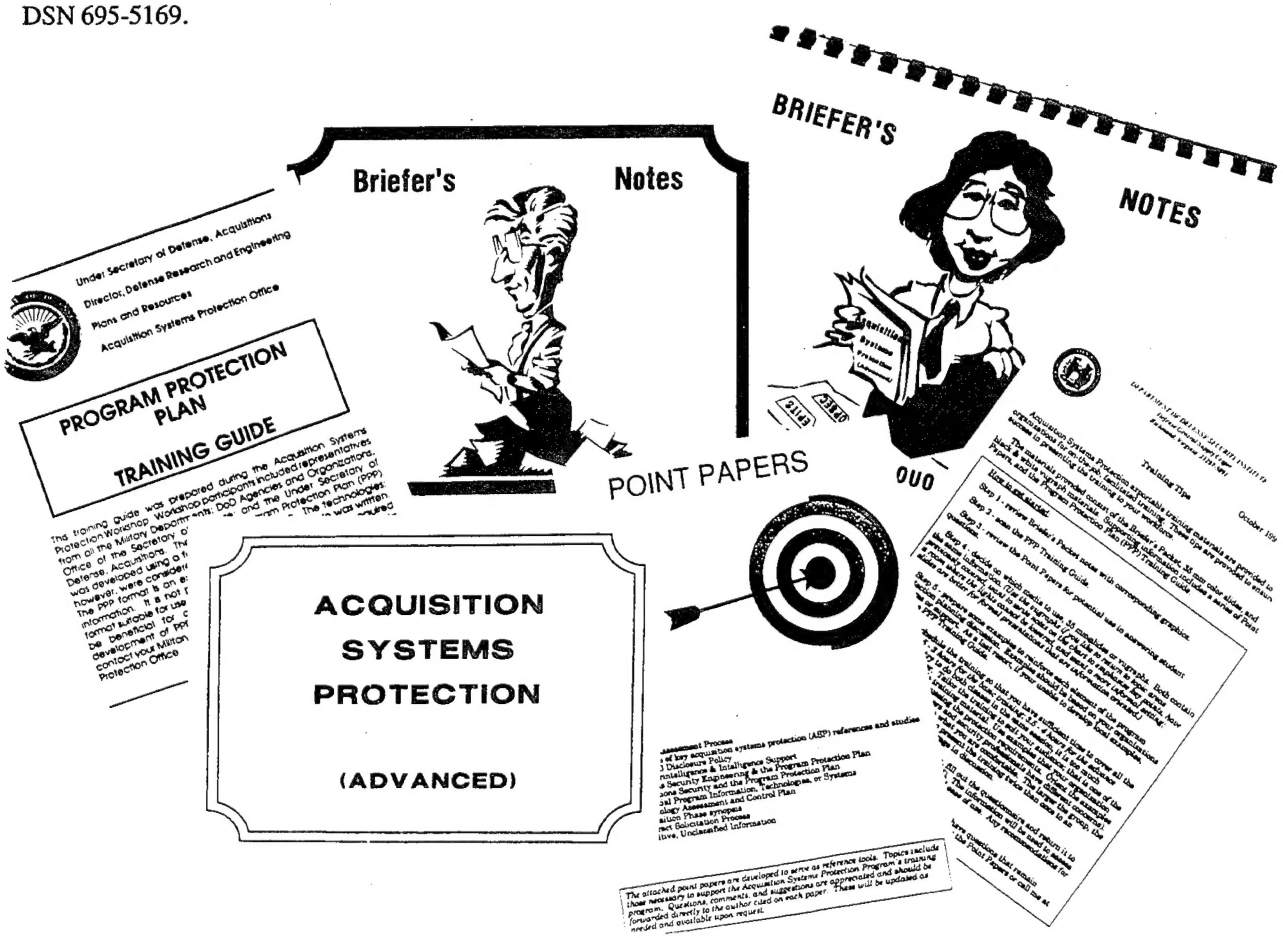
Acquisition Security Modules

A series of exportable training modules on acquisition systems protection for use by presenters at the component, installation, activity, or program level.

- *Introduction to Acquisition Systems Protection*: A 90-minute course of instruction designed to orient personnel on the basics of acquisition systems management and introduce the fundamentals of the protection program.
- *Acquisition Systems Protection (Advanced)*: A 4-hour lesson designed for practitioners developing program protection plans.
- *Acquisition Systems Protection for Acquisition Professionals*: A 90-minute lesson focusing on the enabling disciplines for protection planning such as security countermeasures, counterintelligence support, operations security and intelligence support.

Training tools include videotapes (see page 40) and projected independent study courses.

For more information on these products, contact your organization's protection specialist or security manager. Additional information is also available from the Acquisition Systems Protection Office or the Defense Security Institute, ATTN: Pat Nemanic, 8000 Jefferson Davis Highway, Richmond, VA 23297-5091. Or call (804) 279-5169, DSN 695-5169.



Acquisition Systems Protection

Meeting the Challenges of the New Security Paradigm

by Edward P. Casey

For security professionals, both in government and industry, the 1990s has been a decade of sweeping change. Dramatic shifts in the political and military balance, an increasing focus on economic competition, and the ever more rapid pace of technological advancement have posed serious challenges to a national security infrastructure essentially crafted in the post-World War II era to deal with the Communist threat.

For Department of Defense and contractor security personnel charged with the protection of advanced weapons systems in the acquisition cycle, the introduction to change came early, with the February, 1991, publication of DoD Directive 5000.1, "Defense Acquisition," and DoD Instruction 5000.2, "Defense Acquisition Policies and Procedures." These documents formally established the Acquisition Systems Protection Program (ASPP) within the DoD. With ASPP have come a series of new policies on program protection and technology control aimed at safeguarding U.S. technological superiority, economic competitiveness, and the uncompromising combat effectiveness of U.S. weapons systems.

As the decade advanced, ASPP proved to be on the leading edge of a momentous shift in the entire security community. 1993 saw the signing of Executive Order 12829 establishing a National Industrial Security Program (NISP). Publication of a NISP Operating Manual (NISPOM) and of a new Executive Order on classifying National Security Information (NSI) are anticipated before the end of 1994. Perhaps most significantly, by 1993 the need for fundamental change in the security infrastructure moved the Secretary of Defense and the Director of Central Intelligence to convene a Joint Security Commission charged with developing a new approach to security suited to the challenges of the 1990s and beyond.

The JSC Report

The Joint Security Commission, or JSC, conducted an extensive, community-wide study of the issues and produced an initial report of its findings in February, 1994. The JSC Report, along with a final version published in June, 1994, which incorporated the community-wide response to the Commission's recommendations, are landmark documents for the future direction of our national security efforts. The JSC recommendations are numerous and detailed. In substance, the principal recommendations include:

- the use of a risk management approach, which considers actual threats, inherent vulnerabilities and the availability of costs of countermeasures as the underlying basis for making security decisions.
- a new security policy structure and classification system designed to support risk management.
- the creation of a uniform cost-accounting methodology and tracking system for security resources.
- increased attention to personnel security and information systems security.
- creation of a partnership between government and industry to enhance security, leaving adversarial roles behind.
- a security executive committee, reporting to the National Security Council, to oversee the security system.

The JSC Report has received broad dissemination in the intelligence and security communities and, while several issues require further study, approval for its findings is widespread. The Deputy

Undersecretary of Defense (Acquisition Reform) said, "This office wholeheartedly endorses the recommendations outlined in the JSC Report." Action is already underway to implement many of the JSC recommendations and the Undersecretary of Defense (Policy) chose 38 of the Commission's recommendations for "fast track" implementation within DoD. In concert with the other initiatives, such as the Executive Orders for the NISP and classifying NSI, the changes represented by the JSC recommendations have been called a paradigm shift for U.S. security. At the core of the new security paradigm is the recognition that it is no longer necessary, practical, or cost-effective to attempt to protect every asset against an assumed maximum level of threat or to establish protection standards which are rigid and compliance-oriented instead of flexible and tailored to an assessment of threat, vulnerability, and risk. For the practitioners of ASP, the tenets of the new security paradigm doubtless sounded very familiar, since a risk management approach such as that called for by the JSC is at the heart of ASPP.

ASPP - The DoD View

Although not as widely heralded as the JSC Report, March, 1994, saw the publication of DoD Manual 5200.1-M, Acquisition Systems Protection Program, a document which clearly defined the risk management approach and ASPP. The manual " . . formalized the protection standards and guidance required to prevent foreign intelligence collection and unauthorized disclosure of essential program information, technologies and/or systems during the DoD acquisition process. The goal of the [ASP] program is to selectively and effectively apply security countermeasures to protect essential information, reduce costs, and reduce administrative burdens of security."

According to James M. Baxter, Assistant for Systems Protection in the Office of the Deputy Assistant Secretary of Defense (Intelligence and Security) and the overall ASPP manager, "The ASP concept embodies a very flexible risk management process which closely matches the objectives established in the JSC Report. In addition, ASPP is well-suited to supporting several other recommendations set forth by the JSC. For instance, data to support the cost-accounting methodology for security resources is captured in the Costs section of the Program Protection Plan. Additionally, ASPP is already emphasizing a time/event-phased security classification guide focused on program essential information, such as that called for in the classification system reforms."

Since its initiation in 1991, ASPP has been managed following a three-phased approach to program implementation. The first phase consisted of establishment of the basic ASPP policy and the "marketing" of the concept in the acquisition and security communities within DoD, as well as to defense contractors who would be involved in supporting protection efforts. "The first phase of ASPP culminated with the publication of DoD 5200.1-M," says Mr. Baxter. "In phase two, we are preparing to move on to full program implementation and, in phase three, to provide ongoing advice and assistance to maintain the ASPP effort."

Mr. Baxter sees several objectives for the ASPP as it moves into the implementation phase. "We are working on several issues, such as creating guidance to govern the transition of Special Access Programs into the ASPP environment; the establishment of a horizontal protection database to coordinate program protection and Essential Program Information, Technology or Subsystem (EPITS) data among different programs and services; and the expansion of ASPP-related training courses and supporting materials for field use, this last being an area where the DoD Security Institute is taking the initiative."

"There are a number of challenges ahead for ASPP," Mr. Baxter notes. "Issues, such as more closely integrating ASPP into the overall acquisition reform effort so that it can be used as a means to support the process, are very important. ASPP must also be prepared to deal with supporting such new acquisition concepts as the design of weapons systems that facilitate treaty inspections without compromising EPITS, and the Advanced Concept Technology Demonstrator (ACTD) programs which will greatly accelerate the development and acquisitions process."

Mr. Baxter observes that several of the new security processes associated with both ASPP and the JSC Report will pose one very significant challenge. "In some ways we are really looking at a culture change in the security community.This change will not be easy and will require considerable rethinking and retraining on everyone's part. We in the Acquisition Systems Protection Office will do all we can to help the security and protection community get the job done."

The Service Views - U.S. Army

At the Service level, 1994 has also been a year of important advancements in ASPP. According to James Passarelli, ASPP coordinator in the Office of the Deputy Chief of Staff for Intelligence, Department of the Army, "1994 and 1995 are very busy years for Army ASPP." Since the establishment of the program in 1991, the Army has developed the basic concept, created policies and procedures for implementation, established management and support mechanisms in the acquisitions and intelligence and security communities, and fielded a training program and working aids. "In 1994, the Army is validating the ASPP work done so far and defining our future direction in terms of the many changes currently impacting on both the acquisitions and security environments," says Mr. Passarelli.

While initial Army efforts concentrated on creating a climate to assist preparation of the first round of PPPs, current and future efforts will concentrate on enhancing program implementation and management while continuing to build on the work done to date. According to Mr. Passarelli, "We have a need to emphasize that the PPP is not the end of the process, but really the beginning. The plan is a guide to action, and ASPP does not truly take place until those actions are complete. A big part of the action required by the PPP is the risk management and cost accounting processes called for in the JSC Report. We need to make sure that the countermeasures called for in the plan are in place, cost-efficient, and operating effectively. That sounds simple, but it will be hard work and there are no shortcuts."

This past September, the Army conducted an ASPP workshop in the Washington, D.C. area with service-wide participation. Among the topics discussed were the nature and importance of linkages among EPITS, threat, and countermeasures; obtaining matrix security support and intelligence threat assessments; development of the PPP; the role of Systems Security Engineering (SSE); and future ASPP initiatives. Says Mr. Passarelli, "One of our primary goals is to make ASPP 'value-added' for the Army acquisitions process. We need to view ASPP as representing new opportunities versus new requirements and we are going to focus our efforts on increasing the effectiveness and value of ASPP in this regard."

The Service Views - U.S. Navy

The U.S. Navy takes a similar view, seeing ASPP as a "cost reducer," according to CDR David Johnson, Assistant for Intelligence in the Office of the Assistant Secretary of the Navy for Research, Development, and Acquisitions. "Effective ASPP will save scarce acquisition and operational dollars," says CDR Johnson. "Right now, the Navy is in the process of revising its guidance to reflect the requirements of the new DOD ASPP manual."

According to Philip Bennett, head of the Industrial Security Policy Branch in the Office of the Chief of Naval Operations, "A specific revision included in OPNAV Instruction 5510.1H, Depart-

ment of the Navy Information and Personnel Security Program, is an increasing emphasis on the role of industrial security in its relationship to both ASPP and the requirements of the new NISP. There needs to be a greater linkage between ASPP and the NISP to enhance industry's role and support in the protection process. As many of the savings and improvements in program protection will have to take place in the contractor industrial base in order to be truly effective, the NISP needs to encompass the ASPP philosophy. Industry should be responsible, along with government, for implementing the new efficiencies and cost savings. We need to do a better job of educating industry and bringing them on board."

Both CDR Johnson and Mr. Bennett cite ASPP education and training as an immediate item for Navy emphasis. Navy policy calls for decentralized management of ASPP at the Systems Command level, and it is at that level that ASPP initiatives within the Navy are taking place. "ASPP is beginning to receive increasing Command interest in the Navy," says CDR Johnson. "In order to manage ASPP in the future, we will need to be able to identify and program for the funding, time, and resources necessary to make effective protection an reality. The key to this effort will be educated managers and decision makers with well-trained staffs supporting them." Both also note that there is an increased utility in the threat products received from the Intelligence Community in support of ASPP. Mr. Bennett believes the scope and gravity of the threat "need to be highlighted to acquisition decision makers to facilitate protection planning. Of particular use is the inclusion of data identifying the new critical technologies, along with the foreign collections threat to these technologies, to form a more complete picture of the total threat to specific programs and technologies."

Other areas identified for increasing Navy ASPP emphasis are the need for inter-service coordination and the horizontal protection database, and the refinement of security-related cost-accounting to document ASPP effectiveness and cost savings. Notes CDR Johnson, "For ASPP to advance, the program must have Command interest and support. You get that when you can show efficiencies and cost savings."

The Service Views - U.S. Air Force

In addition to the changes brought about by ASPP, Air Force security practitioners have had to contend with a significant restructuring of their acquisitions environment, with the combination of Air Force Systems Command and Air Force Logistics Command into the new Air Force Material Command (AFMC). The emerging ASPP process has had to be tailored to new and revised Air Force acquisitions programs and processes.

In the words of COL William Kraus, Chief of the Acquisition Policy Management Division and Deputy Assistant Secretary of the Air Force (Management Policy and Program Integration), "New Air Force security priorities are being set within ASPP guidelines. Basic Air Force ASPP policy directives and instructions were issued in late 1993 to conform to the guidelines established in DoD 5200.1-M. For the Air Force, ASPP and program protection planning are all about creating a balance of security disciplines and streamlining the protection process as a part of overall acquisition reform."

As with the other services, the Air Force views education and training as essential to facilitating ASPP. Says COL Kraus, "ASPP represents a culture change. Cultures are changed not by publishing directives and instructions, but by leadership and action. Education and training are necessary both for the leadership, and for the people who

must be the 'doers' of ASPP if they are to understand what is really expected."

"Within the Air Force, AFMC is the prime mover for implementing the new culture change," relates Ted Konduris, acquisition security point of contact within headquarters, USAF Security Police. The Air Force major commands and system operators are being briefed and trained on ASPP by AFMC, and a new manpower standard has been proposed by AFMC which will integrate all the security disciplines into a single ASPP team. Under this new standard, acquisition security positions will also be placed directly in the laboratories to further the ASPP mission. In addition, 200 security data elements are being added to the Air Force acquisitions model computer database to accommodate ASPP planning. Mr. Konduris notes that the Air Force is also currently updating the threat to its acquisition programs overall and is researching ways to build a reliable cost estimate model and database for security-related costs in support of the ASPP effort.

ASPP - A look at the future

As 1994 draws to a close, it is apparent that DoD and the Services are making important strides in implementing ASPP. Further, ASPP is well-suited as a risk management tool for meeting the challenges of the new security paradigm. As recognized at both DoD and service levels, ASPP, like the changes called for in the JSC Report, represents a culture change in which training and education play a pivotal role in preparing the security community for what lies ahead.

Looking to the future, it is apparent that at least in the near term, there will be increasing emphasis on cost efficiency and resource management throughout DoD. This emphasis is recognized in the move to acquisition reform and the need for the security community to support this reform with a realistic cost-accounting methodology and a means for planning and managing required security resources. ASPP addresses this need and is working toward this goal. The risk management process utilized in ASPP will increase cost efficiencies and should increase the effective application of existing security resources.

The same flexibility which allows the ASPP process to extend effective protection to emerging advanced technologies will allow ASPP to accommodate additional changes in security policies and procedures as they emerge from the JSC process. ASPP will be well-suited to manage implementation of mandated changes to the security classification system as they impact on acquisition programs. Similarly, the new policies governing industrial security as promulgated in the NISPOM are closely involved with the acquisition protection efforts to be managed under ASPP.

Farther into the future, other challenges await. The JSC Report made reference to the growing importance of information systems security. As information and its applications grow to the status of a separate element of U.S. national power, and as concepts such as the information superhighway and information warfare are further developed and refined, ASPP will serve as a tool to identify future threat and vulnerabilities and to plan, develop, and manage the effective application of the security countermeasures of tomorrow.

Edward P. Casey is the manager for Special Projects for Beta Analytics International, Inc., in which position he manages and directs specialized security and related services for a variety of government and commercial clients. Mr. Casey has lectured and taught extensively on ASPP topics and has managed and performed program protection planning and other services for numerous acquisition programs in the military services and DoD agencies.

A note from Pat Nemanic

Instructor on Acquisition Systems Protection, DoD Security Institute

Much has been written about Acquisition Systems Protection (ASP) to include the information in DoDD 5000.1 and DoDI 5000.2, but none of what is written provides specific guidance on how to devise acquisition systems protection. Being conscious of this void, I am always on the look out for something that will help make acquisition systems protection easier.

While visiting with Jim Baxter at the Acquisition Systems Protection Office, I noticed a paper he had on his desk, "Exit Criteria for Program Protection Plan (PPP) Approval" list. This list provides some excellent elements to think about. In fact, if you can answer all of the elements on the exit criteria list, you will not only have the basis for a program protection plan and be well on your way to fulfilling the intent of the requirements of acquisitions systems protection but, more importantly, provide protection for your program.

Acquisition Systems Program Protection Plan
Exit Criteria for PPP Approval

A. Describe the System

1. Mission, military value, operational, parameters
2. ID locations, facilities, times where EPITS are used, stored, analyzed, tested.
3. ID unusual factors (e.g., TLI) that increase/decrease intelligence interest.
4. ID supported or supporting programs

B. Describe EPITS (Essential Program Information Technology Systems)

1. ID technical parameters that, if compromised, would reduce combat effectiveness of system life.
2. Establish criteria for what constitutes loss of information.
3. ID EPITS of supporting programs.
4. Describe how compromise/loss of support program EPITS would affect the program.
5. ID unique production/fabrication techniques whose loss/compromise would endanger EPITS.

C. Describe Threat and Vulnerability Analysis

1. ID countries/organizations with interest/capability to collect program information.
2. ID foreign research on EPITS and level of sophistication.
3. ID how foreign research is being protected.
4. When, where, how will EPITS be vulnerable to threat?

D. Describe the Countermeasures (CM)

1. ID whether time or event driven (implementation/termination).
2. What is the project manager's (PM) security concept and level of protection?
3. How will assets be deployed to counter vulnerabilities?
4. Provide cost-benefit analysis and justify security concept.
5. How will supported/supporting programs' EPITS be protected?
6. How will PM measure CM effect and update/validate concept?

E. Describe Cost Criteria

1. Provide cost data by Acquisition Phase.
2. Break down security costs by discipline.

F. Describe the SCG

1. How will EPITS be classified, marked, distributed, and controlled to limit flow?
2. What criteria will determine if classification level should be reduced/eliminated?
3. Does the SCG correlate with the identified EPITS?
4. Justify any indefinite classification period.

G. Describe the Technical Assessment Control Plan (TA/CP)

1. Describe the system, mission , and military value.
2. ID technology (EPITS) critical to the system and value to U.S. military capability.
3. ID probability of compromise and likely damage to military capability and/or industrial base if EPITS are lost.
4. Include delegation of disclosure authority letter (DDL) that provides guidance on joint ventures.

H. Describe System Security Engineering (Milestone II and later only)

1. ID threats and vulnerabilities of system in its operational environment.
2. ID design features that ensure effective security in operational environment.
3. ID changes to fielded system which would allow export.
4. Outline methodology for achieving SSE goals, by acquisition phase.

The Acquisition Systems Protection Program and the System Protection Concept

by Major Robert Newton, USA
ASPO, Office of Assistant Secretary of Defense

Since the end of the Cold War, changes within the counterintelligence and security community have occurred daily. As professionals, we're responsible for keeping up with the major changes and analyzing how those changes may or may not impact the commands or activities we serve. One of the more significant changes to how the DoD goes about the business of procurement is the advent of the Acquisition Systems Protection Program or "ASPP." The ASPP is already transforming the acquisition process by introducing a new approach in the protection of essential DoD program information and technologies. If your command or activity is involved in weapons or combat systems procurement, and this is the first you've heard about ASPP, you're well behind the power curve. It's time to get smart! The author is with the Acquisition Systems Protection Office which is charged with developing standard acquisition systems protection policies and procedures for the DoD.

The Acquisition Systems Protection Program (ASPP) was developed in response to recognized shortcomings in the acquisition, intelligence and security communities of the Department of Defense (DoD). Several DoD studies indicated the U.S. had difficulty protecting our most sensitive technology and information from compromise. With the demise of the Cold War, this problem has not disappeared with the Soviet empire. Technology transfer, co-production, and co-development programs could increase the risk of compromise of critical technology if proper safeguards are not imposed. This Acquisition Systems Protection (ASP) concept is based upon the tailored application of countermeasures to specific threats and vulnerabilities of an acquisition program. This produces a cost-effective, secure environment for DoD critical technology throughout the procurement process.

The ASP program is established under authority of DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," and DoD 5200.1-M, "Acquisitions Systems Protection Program Manual." Part 5, Section F of DoD Instruction 5000.2 requires development of a Program Protection Plan (PPP) for every DoD acquisition program and that it be updated prior to each Milestone Review.

In January of 1991, the Acquisition Systems Protection Office (ASPO) was established by memorandum from the Under Secretary of Defense (Acquisition) with responsibility to develop standard ASP policies and procedures for DoD. In addition, the ASPO was given authority to review and approve all PPPs. With the release of DoD 5200.1-M, a complete guide on the ASP program and development of PPPs is now available to all users.

The core of the ASP concept and development of the PPP is identification of Essential Program Information, Technology, or Systems (EPITS) for each acquisition program. EPITS are the most important pieces of technology, manufacturing processes, basic research information, or support equipment which give a particular weapon or system its special capabilities that allow it to perform its combat mission successfully. The identification of EPITS is usually the job of engineers assigned to a program; however, the program manager is ultimately responsible for final selection.

Once EPITS are identified, the security and intelligence communities become involved. For ex-

ample, a program manager responsible for a program must request a counterintelligence analysis to identify which countries have an interest and the capability to collect information on the identified EPITS. This is where the security professional steps in.

When this analysis is returned to the program office, security specialists assist program managers in identifying the program's vulnerabilities, probability of compromise, and the countermeasures that should be used to protect the program. Although security specialists are responsible for advising the program manager on these matters, the actual selection or rejection of the countermeasures is based upon a cost-benefit risk analysis by the program manager. The goal of the ASPP is to manage risk to the program cost-effectively, not to ensure absolute protection from all threats.

A critical ingredient of the ASPP is development of the Program Protection Plan (PPP). The PPP is a single source management plan for security of the system throughout its life cycle. Consisting of a Technology Assessment/Control Plan, a time- or event-phased Security Classification Guide, and a System Security Engineering Management Plan (which concentrates on design specifications to protect the system in its operational/combat environment), the PPP is a living document requiring regular updates. As a minimum, the PPP must be updated and approved prior to each Milestone Review.

In conclusion, the continued loss of critical technology, the reduced competitive position of U.S. industry, and the need to significantly reduce the cost and administrative burdens of security, demand a new approach to the protection of our new weapons programs. The post-Cold War era will not allow us to protect our systems based upon a "worst-case" scenario. On the other hand, eliminating or haphazardly reducing protective requirements fails to protect the defense industry from economic espionage by other nations and increases the risks to our military forces.

The ASP program is the sensible compromise which ensures protection of our most essential technology from friends, foes, and competitors so that the U.S. can assert a technological lead well into the 21st century.

Reprinted from the Naval Criminal Investigative Service's Sentry magazine, Winter 1993-1994 issue.

Program Protection Plan (PPP)

The PPP is oriented towards protection of the most critical elements, not an entire system:

- Identified as Essential Program Information, Technologies, or Systems (EPITS)
- Goal is to improve the protection of the most important elements of the program while reducing the overall cost and administrative burden of protection.

Questions and Answers about

Intelligence threat assessments for developing a risk analysis

Ruth Ann Jones is the Acquisition Security Program Manager for the National Aero-Space Plane (NASP) Joint Program Office and for the Hypersonic Systems Technology Program (HySTP). She was one of the first to successfully develop and implement the program protection and technology control requirements of the DoD 5000 series. As a guest speaker and session leader for the ASPO conferences, Ms. Jones has shared her expertise with many of today's key senior DoD acquisition leaders and program managers. She has been commended by the counterintelligence community for her work in developing an effective system threat assessment process for acquisition programs.

In this interview with the editor assuming the role of a program manager, Ms. Jones offers us some clear guidance based on her experience in developing a risk analysis and program protection plan for the NASP program based on a threat assessment.

Q. *Ms. Jones, who or what organization should I contact for an intelligence threat assessment with regard to my program?*

A. Since you are looking for a program threat assessment, you should contact your servicing Counterintelligence Office. You need to know the nature and scope of the threat the program faces during the acquisition process. Your local counterintelligence folks will respond to your call and assist you in the development of your request for service. Your Intelligence Office provides the system threat assessment - the threat to the system in its projected operational environment, supporting the development of the System Threat Assessment Report or STAR.

Q: *The identification of a servicing CI office might be self-evident for most program managers particularly if they belong to a particular military service. But what if my weapon system falls under a joint program?*

A: Of course each military service has its own intelligence and counterintelligence organization. For joint programs the servicing counterintelligence organization will be specified in the MOA (memorandum of agreement) that establishes the program.

Q. *What should my request include? Should I list the EPITS?*

A. Your EPITS list is a part of your request for service. You will also have to list each of your contractors (and sub-contractors if they will be handling any of your EPITS) to include addresses and points of contact. Additionally, the name and address and point of contact for each laboratory, research facility, test and evaluation facility and any grantees (usually universities) who may have access to your EPITS will have to be shown.

Q. *How should I communicate this request - by memorandum, electronic message or by telephone?*

A. Begin with a phone call to your local Counterintelligence Office. Set up a meeting in your office to discuss the nature of your program with members of their staff. It is important for them to be familiar with your program so they can make efficient comparisons with similar efforts in the international technological community.

Q. *Should I as the program manager or security specialist be the one to make this request or should I go through a Counterintelligence professional?*

A. You make the phone call and you set up the initial meeting. The exact format of your request for Counterintelligence service is established by your local Counterintelligence Office. Some have developed worksheets to help you assemble all necessary information for your request. Some requests are made on a form known as an Intelligence Production Requirement or IPR. Other requests are in a letter format which is signed out by your program director. Either will get your request into the counterintelligence system.

Q. *What should I expect to receive as a result of this request for a threat assessment? Will it name countries and intelligence collection methods?*

A. Your Program Threat Assessment report will validate your EPITS list by identifying what you have that someone else wants. It should identify the adversary by country, program, and contractor. The report will also describe the most plausible methods of adversary collection and list locations where known adversarial collections have been or are being made relative to your program.

Q: *This sounds like rather sensitive information. I assume that it would be a classified report. But does that mean that the products that follow such as the risk assessment and the program protection plan itself have to be classified at the same level?*

A: Yes, the threat assessment will be classified. But the subsequent risk analysis and other products would not contain the classified information in the assessment. There may be exceptions, however, based on previous classification guidance. Normally, everything but the threat assessment would be marked as FOUO (For Official Use Only) and handled appropriately.

Q. *What is a reasonable time to wait for this assessment?*

A. Tough question. If you have a normal system program office with a fairly normal system concept, the report should take 90-120 days. If you are developing warp drive, a cloaking device, or something equally unique, it could take a little longer. These reports are fairly new and the counterintelligence community is focusing its efforts on delivering a product that meets the needs of their customers. Everyone is working hard and the process seems to get better with each request. Be patient — don't sacrifice quality for an unreasonably short suspense.

Q. *Upon receipt of an intelligence threat assessment for my program, what is my next step in the development of a PPP? What am I supposed to do with this threat information?*

A. You and your staff of technologists, engineers, researchers, and Program Managers will conduct the risk analysis assisted by your local Acquisition Security Directorate, Foreign Disclosure Office and Counterintelligence Office. This risk analysis asks the question, *"If this is what I have that is of value and this is who wants it — what is the impact if I just give it to them?"* A couple of useful documents must be available to you during the risk analysis. A current copy of your security classification guide, the International Traffic In Arms Regulation (ITAR) and a copy of the Militarily Critical Technologies List (MCTL) will help you identify those EPITS which may be classified under certain conditions and/or subject to U.S. Export Control Laws. Once your risk analysis has been completed and approved by your program director, you are ready to begin the development of your program protection plan. It is the program protection plan that will define and describe the countermeasures to be applied to protect specific EPITS at specifically identified locations during the acquisition process.

Proceedings of the conference on ...

PERSEREC

Computer Crime: A Peopleware Problem

Published by the Defense Personnel Security Research Center, Monterey, California. Now available through the Defense Technical Information Center.

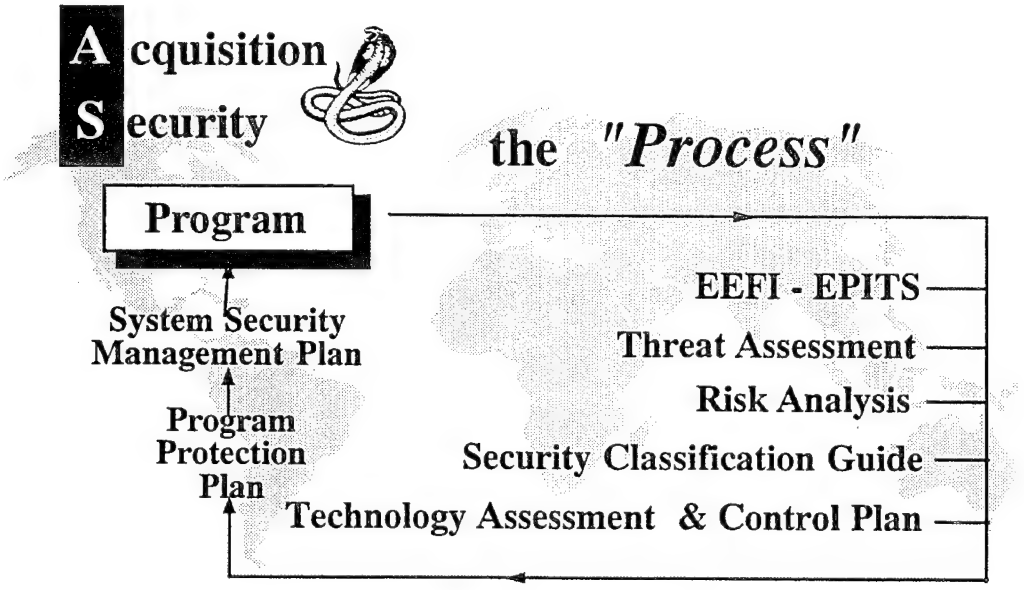
To obtain a copy, ask for DTIC report number AD-A281541.

If you do not have a DTIC account call:

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, VA 22060-6218
(703) 767-8273, DSN 427-8273

If you *do* have an account, call (703) 767-8274, DSN 427, 8274

The **Acquisition Security Program Management Process Chart** begins with a category shown as EEFI-EPITS. Essential elements of friendly information (EEFI) are the vulnerabilities of the present or new system which limit the ability of the system to execute its mission requirements in the current or projected operational environment. Essential program information, technologies, and systems (EPITS) are the technologies which will be developed and applied to the present or new system to eliminate or greatly reduce the vulnerabilities. EEFI and EPITS are two separate issues. EEFI are a product of the intelligence system threat assessment. EPITS, developed to limit EEFI vulnerabilities, are developed by the System Program Office and validated by the program threat assessment. EEFI have historically been protected by the application of the operations security (OPSEC) process and other traditional security actions. These development processes are a part of acquisition program risk management. Risk management cannot be accomplished in a vacuum, one of the many reasons that acquisition security program management must be seen as an element of program management.



Acquisition Security Directorate

- The ASC acquisition security process was developed by a team of experts from the Air Force security community led by ASC security personnel.

- Our staff worked with senior Department of Defense, NASA, and DoD contractor acquisition experts to establish an acquisition security process which meets the needs of our customers.

- The process is managed in real-time and is designed to be flexible so as to forecast and quickly respond to today's rapidly changing international environment.

DoD Acquisition Systems Protection Program

DoD documents:

a. DoD Directive 5000.1, *Defense Acquisition*, February 23, 1991, Part 1, paragraph B5.

b. DoD Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, February 23, 1991, Part 5, Section F, and Part 6, Section J.

c. DoD 5200.1-M, *Acquisition Systems Protection Program*, March 16, 1994.

d. *Intelligence Collection Capabilities Matrix (U)*, Defense Intelligence Agency, DIW-2400-731-93, March 1993, SECRET/NOFORN.

e. *Foreign Interest in U.S. Critical Technologies Matrix (U)*, Defense Intelligence Agency, PC-1830-14-93, November 1993, SECRET/NOFORN/WINTEL/NOCONTRACT.

f. Air Force Policy Directive 31-7, *Acquisition Security,* March 2, 1993.

g. Air Force Instruction 31-703, *Product Security*, February 7, 1994.

Articles and periodicals:

a. Casey, Edward P., "Acquisition Systems Protection," Program Manager, May-June 1992, page 14.

b. Newton, Robert (Captain, USA), "Protecting the U.S. Technical Lead," Army RD&A Bulletin, March-April 1993, page 21.

c. Newton Robert (Captain, USA), "The Acquisition Systems Protection Program and the System Protection Concept," *Sentry*, Naval Criminal Investigative Service, Winter 1993-1994, page 11.

d. "The Acquisition Systems Protection Program," *MRTFB Gazette*, OUSD(A&T(DT&E, April 1994, page 4.

e. Special issue of the *Security Awareness Bulletin*, DoD Security Institute (DoDSI), April 1993.

f. Issues of the *ASP Angle*, published periodically by the Acquisition Systems Protection Office.

Training courses and materials:

a. Course module, *Introduction to Acquisition Systems Protection*, 4 hours, DoDSI.

b. Course module, *System Protection for the Acquisition Professional,* 1.5 hours, DoDSI.

c. Course module, *Advanced Acquisition System Protection*, 4 hours, DoDSI.

d. Video, *ASP Executive Overview,* 13 minutes, DoDSI, May 1993.

e. Video, *Protection Planning,* 23 minutes with instructor's guide, DoDSI, December 1993.

Contacts:

ORGANIZATION	CONTACTS	OFFICE	PHONE NUMBER
OSD	Doug Cavileer Jim Baxter Rene Davis-Harding	ODASD(I&S)	(703) 695-2686
Army	Jim Passarelli	DAMI	(703) 693-5233
Navy	Cmdr Dave Johnson	OASN(C4I/EW/SPACE)	(703) 614-4691
Air Force	Col Bill Kraus Ted Konduris	SAF/AQXA AF/SPI	(703) 697-6093 (703) 697-9470
BMDO	Col Bob Peavey	SIS	(703) 412-3493
DIA	Nick Bennett Frank Fishbaugh	PAN-2 PGT-1	(202) 373-4752 (202) 373-8278
NSA	Charles Malinowski	N22	(301) 688-7674
DoDSI	Pat Nemanic		(804) 279-5169

No Funny STU-III Stories

by Wayne Lund, Instructor
Department Of Defense Security Institute

I was sitting in a meeting yesterday, when one of the senior members of our staff (I call him "Sir") turned to me and said, "With all the STU-III classes that you have given, I'll bet you have heard some funny stories about the STU-III. You ought to write an article for the *Security Awareness Bulletin* and include all the funny STU-III stories that you have heard."

"No, Sir," I responded. "I have not heard any funny STU-III stories. I have only heard of a lot of offices that have STU-III's that never get used."

I thought to myself, I could write funny stories about my two puppies, Freckles and Chelsea, but not about a telephone. (The puppies really belong to my wife and kids. I just pay the vet bills and fill in the holes that they dig in my back yard.)

It's just a telephone.

In all fairness to Sir, I have heard some stories of the sort that I think he was talking about. I just don't think they are very funny. You see, to me a STU-III is just a telephone. It is a special telephone that allows us to have classified conversations without fear of interception, but it's still just a telephone. I have never been particularly interested in gadgets (to include fancy telephones). I am only interested in what a gadget can do to make my life simpler or more enjoyable. I think Sir is more technically oriented than I am. Since I'm not particularly interested in gadgets, stories about people's problems with these devices don't strike me as funny.

I'm really more interested in planting azaleas than I am in hearing about the problems that people are having with their telephones. I could tell you a funny story about the time I planted a beautiful purple-blossoming azalea bush next to my garden shed. When I came home from work the next day I found a hole where the bush had been. Freckles came running out to greet me and Chelsea came running up behind her with what was left of my new azalea bush in her mouth!

No funny stories about the regulations.

Sir probably assumed that I have heard stories about people who are confused about the rules and regulations related to use of the STU-III. He's right. I have heard of some confusion. I just don't think that confusion about regulations is funny. Here, too, Sir and I each have a different frame of reference. Sir is a retired Army Colonel. He takes rules and regulations very seriously. I, on the other hand, was an unemployed social worker who got into the security business 15 years ago because I needed a job.

Don't get me wrong. I realize that rules are necessary. They establish order and create a system with which we can accomplish our goals. I'm just not fascinated by rules. I think of them the same way that I think of gadgets. I only like rules for what they can do for me (or for us as a society). Rules should serve a purpose; e.g., We have a rule that Freckles and Chelsea must stay inside my fenced backyard so they will not dig up my neighbor's bushes.

Much of the confusion about STU-III rules comes from the fact that they are based on the rules that were established for traditional secure communications (COMSEC) systems; but the STU-III rules are in many ways much less restrictive and cumbersome than the rules governing the older systems.

The old COMSEC rules were very restrictive and cumbersome for good reason. If an adversary somehow obtained the code (or key) that we were using to encrypt our secure message traffic, an intercepted message could be deciphered. With the older systems the key was usually loaded into the

secure communications device in some physical form such as a punch card, or paper tape with a pattern of holes punched in it . (It was this type of key material that the Walker spy ring specialized in selling to the Soviet Union.) Any key material that is in a physical form is very susceptible to compromise.

It is unfortunate that some people who are somewhat familiar with the strict regulations associated with traditional COMSEC systems avoid using STU-III equipment because they want to avoid cumbersome regulations. The rules related to the STU-III program are really quite simple.

Why STU-III regulations are simpler

Advancements in technology have allowed us to develop the STU-III products, which actually generate a traffic encryption key at the time that a secure call is made. Since the traffic encryption key did not exist prior to the call, it only exists in electronic form, and disappears when the call is terminated, it is extremely unlikely that an adversary will be able to obtain the key. Even if that did happen, the key could only be used to decipher that one message, since a new traffic encryption key (code) is generated for each call.

There is more to the protection of STU-III key than that. The STU-III system is set up with a multi-tiered system of key protection including Seed Key, which is used to initially set up your STU-III phone; and Operational Key, which remains resident in the memory of your STU-III phone and serves to protect the initial portion of the call during which time the Traffic Encryption Key is generated. Seed Key and Operational Key also contain your local office's identification information which can be viewed by the other party when you make a secure call.

We have already bought them, now let's use the darn things!

Chelsea looks like a half-sized English Sheep Dog. Her sister, Freckles is almost bald, like me. Last spring we went out and bought electric dog grooming sheers with all the fancy attachments so I could give Chelsea a haircut. There is no way that this poor dog could survive the infamous heat and humidity of the Richmond summer without a haircut! The sheers are very well designed, and I'm sure they are worth every penny of the $49.98 that we paid for them. The sheers could be used hundreds of times, and with doggie haircuts going for $15 - $20 at the pet store, the sheers would soon pay for themselves.

The problem is this. The first time I used the sheers I scalped Chelsea so drastically that she made Freckles look like a fluffball. I accidentally pinched her ear in the clipper, and for weeks after that haircut Chelsea would run and hide under the deck whenever she saw me coming her way. She looked so bad that my family would not speak to me until November when her fur started growing back. I thought I would never give that dog a haircut again!

When the weather started getting hot last spring my wife reminded me it was once again time for Chelsea to have a haircut. I considered the trauma of my first attempt and was tempted to just take her to the pet shop and pay for her haircut. Then I started reading the instructions that had come in the package with the clippers. They explained how to use the attachments to avoid clipping the hair too short, and how to avoid pinching the dog's ears. I decided to try it again. Chelsea's haircut this year looked great! The $49.98 that we spent for the sheers would have been money wasted if I had decided not to use them again. Once I read the directions and gave myself a second chance I found the job to be quite simple.

A STU-III phone is a bit more expensive than a pair of dog-grooming sheers. Each unit costs about $2000. These are a good investment if they are used as intended. What troubles me about this investment is that there are many STU-III units that are never used in the secure mode. Some are only used as plain old telephones. Others remain packed in the box that they came in and are not used at all. The U.S. Government and government contractors have purchased about 263,000 STU-III units. At $2000 each, we have an investment of over $500 million just in the phones. We also have a substantial investment in the key management system and administrative systems that support the STU-III program. If the phones are used this is

money well spent. If they are not used it is money wasted. I hope the STU-III phones in your office are being used.

How does using the STU-III save money?

Without secure communications, the only appropriate way to have a secure conversation with someone about matters that are classified or sensitive is to have a meeting. If the other person is in the same city as you, it may take you an hour's driving time, find a parking place, and go in for your meeting. After the meeting it will take you another hour to get back to your office and back to work. If the other person is in another city, the travel time could amount to a day or two, plus you have the added expense of travel costs. If your time is worth anything to your organization, saving time is saving money. With the availability of the STU-III you may have your conversation with none of the associated travel costs of time or money. You may be able to avoid taking unnecessary business trips by accomplishing your business over the phone. From a personal standpoint this means you will not have to spend so much time away from your home and family.

The cost of lost information

People talk on the phone. People have discussions about sensitive information on the phone. Even if they are not supposed to, some people discuss classified information on the phone. What these people apparently don't realize is that when they have these discussions the chances are great that someone is listening in.

Everyone in our organization must be aware of just how easy it is to listen in on a telephone conversation. They should know that specific phones such as those at a cleared facility are often targeted, and that modern eavesdropping equipment allows the adversary to queue in on specific types of information.

We must convince people that the information they discuss over the phone is indeed vulnerable.

Losing control of sensitive or classified information is significant. We often speak in general terms about protecting National Security. This general term includes protecting our country's military, economic, and diplomatic interests.

To be meaningful to most employees it may help to personalize the concept. Think of the military threat in terms of human life. Lost information could cost the lives of U.S. servicemen and women as well as the lives of civilians.

The economic threat of losing our technological edge is quite apparent. As foreign firms acquire our technology, they attempt to take over the market — costing many Americans their jobs. The jobs of your company's employees may also be dependent upon protecting information about corporate financial matters, pricing strategies, and marketing plans.

The disclosure of classified information may also have an impact on the diplomatic stance of the United States. This is sometimes less obvious to those of us who handle classified information.

Cost of not communicating

In contrast to the problem of not protecting information, we also experience problems when those of us who are working together fail to communicate. This can result in missed deadlines, lost sales, duplicated efforts, wasted money, time, and resources.

One of the lessons learned from our involvement in Operation Desert Storm was that we need to streamline our security procedures in such a way that we can adequately protect valuable information while still making that information available to those people on our side who can use it.

We have lots of good reasons to use the STU-III. Why do some people still avoid using it?

People avoid doing things that subject them to additional administrative requirements. We must get the word out that using the STU-III is simple, and we must do everything we can to make it convenient.

Once people realize the risks of making non-secure phone calls and realize how simple it is to

use the STU-III, they will not only be willing to use it, they will insist that they have a STU-III available for their daily use.

No funny stories about the KSD-64A

The KSD-64A is the little black plastic thing that is shaped like the key to your car. When you put the KSD-64A into a hole in your STU-III it can change the STU-III from a plain old telephone into a secure telephone. There is some confusion about the KSD-64A because it is used for several different purposes.

The KSD-64A contains an electronically-erasable-programmable-read-only-memory chip (EEPROM). This device is used to store Seed Key. It can be used as a "Crypto Ignition Key" (CIK) in which case it stores an electronic password which allows you to use the secure features of a particular STU-III. The KSD-64A can also be used as a "Master CIK", which means it contains a special password that not only allows you to use the secure features of your STU-III, but also allows you to change some of the optional settings on your phone. (In some unusual circumstances the KSD-64A is also used to store operational key.)

Since the KSD-64A is reusable, the same device (the same piece of plastic) may be treated differently depending on what information is stored on it at the time. There are different rules concerning the protection of the KSD-64A depending on what it is being used for.

When I am not planting azaleas or filling in holes in my yard, I like to brew my own beer. I reuse old soft-drink bottles by filling them with my latest batch of home-brew. A couple of times I have attempted to make root beer. (I have some funny stories about bottles exploding and scaring the wits out of Freckles and Chelsea.) As with the KSD-64A, I have different rules concerning the protection and storage of the bottles, depending on what they contain.

Secure data devices

As I mentioned earlier, I am not particularly interested in gadgets. I'm only interested in what they can do for me. All that I know about computers is that my P.C. makes it much easier for me to write about my dogs and to check my spelling. I know that computers can talk to each other over telephone lines and that with a STU-III at each end they may do so in a secure mode. Most STU-IIIs allow secure transmission of voice or data.

The first STU-IIIs on the market in about 1987 transmitted at a rate of 2400 bits per second (2.4 baud). By 1990 most STU-IIIs on the market transmitted at the rate of 4.8 baud. The newest STU-III units transmit at the 9.6 baud rate. This higher transmission rate gives much better voice quality, and allows the STU-III to support the use of FAX machines and even Video Docking Units in the secure mode. The higher transmission rate is also significant to computer users because it allows computers to exchange information more quickly. There are some STU-III products available called Secure Data Devices that do not have voice transmission capability, but can support data transmission at the 9.6 or even the 14.4 baud rate.

No funny stories about technical problems

I have heard stories about people having problems with their equipment, uh-h-h ... telephone equipment. (Not funny stories, just stories.)

All three STU-III manufacturers have help lines to respond to technical problems. The numbers are as follows:

AT&T	1-800-243-7883 (919) 279-3411
Motorola	1-800-922-7883 (602) 437-2822
GE / RCA	1-800-521-9689 (609) 727-5282

(Martin-Marietta Corporation provides service for GE / RCA STU-III products.)

Three common technical problems related to the STU-III are:

1. Accidental zeroizing

When the zeroize button on your STU-III is pushed, all of the key information and local identifying information which is stored in the memory of that phone is erased. Sometimes a loss of electrical power may also cause the phone to zeroize. (There is a battery in each STU-III to supply back-up power.) Don't panic. You can load new seed key into the STU-III in just a few minutes. The trick here is to have a small inventory of seed key on hand to use when a phone is accidentally zeroized.

2. Compatibility with digital telephone equipment

STU-III units are designed to be compatible with analog telephone systems. Much of the newer telephone equipment is digitally based, rather than analog based. You may have digital switching equipment in your office building. To make the STU-III compatible with the digital equipment you may need to have an analog card installed in the switching equipment, or you may have to use a device which converts the analog signal from the STU-III to a digital signal. Since digital switching equipment is so commonly used, the manufacturers of STU-III products have developed several solutions to this problem of compatibility.

3. CIKs not being recognized

Sometimes a STU-III does not recognize a CIK even though the CIK is associated with that STU-III. Often this is the result of the CIK being dirty. As a first step, you may try cleaning the contact points of the CIK with your fingernail or some similar item. If after cleaning the CIK it still doesn't work, you may need to zeroize it and make a new CIK. (In most cases you can reuse the same KSD-64A.) If you cannot get a CIK to work in the phone that it is associated with, you should use the Master CIK to delete the malfunctioning one from the keyset.

Unclassified, but sensitive, discussions

If you have a STU-III, you and the people in your organization should get in the habit of using its secure features not only for classified conversations and transmissions, but also for unclassified conversations or transmissions of a sensitive nature. Information about your company's new products, marketing plans, pricing strategies, executive travel plans, corporate financing, etc., is worth protecting. Protecting unclassified, but sensitive, information is a good habit for all of us to develop. For some organizations this concept is more formalized in the form of an OPSEC plan.

You may also have a legal or moral responsibility to protect personal information about your employees. Think of what your competitor could do with the information that passes between your corporate headquarters and your divisions or field offices.

Why am I interested?

Since I have told you that I am not interested in gadgets like fancy telephones, or in the fine points of rules and regulations, you may wonder why I spend my time writing articles like this or teaching a class about the Secure Telephone. The reason is two-fold.

First, I like to see efficiency in government and in industry. Use of the STU-III can yield great savings by providing a low cost system of secure communications.

Second, I am a strong believer in the axiom that knowledge is power. Because of this fundamental principle, I respect the value of sound information security. Protection of information can give us a significant advantage in military, law enforcement, economic, and diplomatic scenarios.

Military analysts agree that it was the technological superiority of the United States and the coalition forces that led to a quick and decisive victory in Operation Desert Storm. Part of that technological superiority was the secure communications capability which we had by using STU-IIIs. Use of the STU-III before, during, and after that conflict allowed us to protect our technological edge.

Sources of information about the STU-III

One of the best ways to get clear guidance on policy is to read the policy yourself. Here's where to look.

Anyone who is involved in ordering STU-III key should be familiar with the following National Security Agency (NSA) publications.

1. Electronic Key Management System Services (EKMS-702.03)
2. Electronic Key Management System Registration Manual (EKMS-702.04)
3. Electronic Key Management Key Ordering Manual (EKMS-702.05)
4. Electronic Key Management System Accounting Manual (EKMS-702.06)

You may obtain these publications from:

EKMS Central Facility
P.O. Box 718
Finksburg, MD 21048-0718.

If you work for a cleared contractor you should be familiar with Chapter 13, Section 9 of the Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M), and the COMSEC Supplement to the Industrial Security Manual (DoD 5220.22-S). You may obtain these documents from your DIS office.

DoDSI's STU-III Handbook for Industry was written to assist cleared defense contractors by summarizing STU-III concepts and policy. Although it is based on policy as it relates to contractors, it has been found to be helpful to other STU-III users. If you would like a copy of this handbook, call me (Wayne Lund) at (804) 279-3939.

Army STU-III policy is published in Security Procedures for the STU-III (Department of the Army Pamphlet 25-16) You may obtain this publication from US Army Communications Electronics Command, Communications Security Logistics Activity, CDR USACCSLA, Attn: SELCL-KPD-OR, Fort Huachuca, AZ 85612-7090

U.S. Air Force COMSEC Custodians may find STU-III accounting policy in the AF COMSEC Accounting Manual (Regulation: AFKAG-2). For information contact U.S. Air Force Cryptologic Support Center, Electronic Security Command, Attn: MMIA, San Antonio, TX 78243-5000, phone (210) 977-2325

Navy, Marine, and Coast Guard STU-III policy is published in the STU-III COMSEC Material Management Manual (CMS 6) which is available from: Director, COMSEC Material System (DCMS), 3801 Nebraska Avenue, N.W., Washington D.C. 20393-5252, phone (202) 282-0311

Training opportunities

Hands-on STU-III training is available from the GSA INFOSEC Training Center in Kansas City, Missouri. Courses are offered in Kansas City, Washington DC, and San Francisco and may be presented at your location on a case-by-case basis.

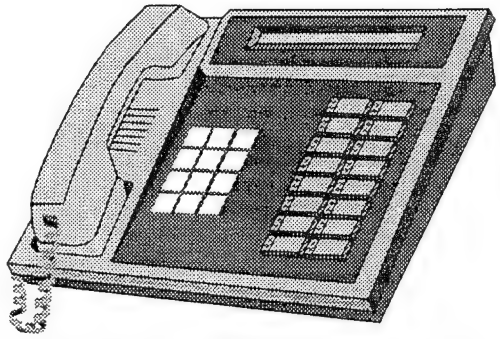
For information contact: GSA INFOSEC Training Center, Registrar's Office, 1500 East Bannister Road, Kansas City, MO 64131-3087, phone (816) 926-7682

"Introduction to the STU-III" is a one-day course which is held at DoDSI in Richmond, Virginia, on the following dates.

This course is also presented at locations around the United States when it is hosted by an organization such as an Industrial Security Awareness Council (ISAC) or by a military or DoD office. Call Mike Black at (804) 279-4187 or Wayne Lund at (804) 279-3939 for more information. If you would like to enroll in one of the classes listed below, please fill out and mail in the Registration form following page 28. The DoDSI Registrar phone number is (804) 279-4891 if you have a question about registering.

December 8, 1994	June 5, 1995
January 12, 1995	August 10, 1995
February 27, 1995	September 18, 1995

Introduction to the STU-III



This one-day course includes an overview of the STU-III program, practical exercises in ordering seed key, and hands-on exercises with STU-III phones. Students are also provided the latest new product information from the manufacturers of STU-III equipment.

The course is ideal for COMSEC Custodians of STU-III Only COMSEC Accounts (SOCA's) and for people who are not COMSEC Custodians but have some responsibility for STU-III units at their work site. The course gives new STU-III users basic guidance in how to use the STU-III and what security responsibilities they have.

Course dates in Richmond, Virginia:

January 19, 1996
March 1, 1996
May 1, 1996
July 1, 1996
September 6, 1996

To enroll in a class, complete and mail the registration form following page 28.

To host Introduction to the STU-III at your location, call Wayne Lund at (804) 279-3939, DSN 695-3939.

You Can Host These Courses On-site at Your Facility (Industry or Government)

Train-the-Trainer Course (TTT) 5220.13A, 4.5 days

Purpose: To train you to *teach* the SBC. This workshop, conducted on the 2 days before a scheduled SBC, prepares you to be an instructor for the SBC. You will receive instruction by DoDSI staff on how to:

- use the SBC materials;
- present selected lessons in the SBC;
- facilitate the preparation of briefings;
- conduct practice briefing sessions; and
- evaluate live briefings.

Under DoDSI supervision, you will then spend the next 2.5 days teaching your first SBC.

Security Briefers Course (SBC) 5220.13, 2.5 days

Purpose: To improve your effectiveness as a security education briefer. You will receive instruction on how to:

- prepare a briefing plan;
- design and use briefing aids;
- present your briefings in a clear and interesting manner; and
- evaluate live briefings.

As the "Security" in the course title suggests, the briefings presented by you in class must address security requirements, but the real emphasis of the course is on accomplishing the above objectives so that you become more skilled and more comfortable at speaking in front of others.

If you are considering participating in the TTT, it is suggested that you: Be responsible for your organization's security briefing program; be an experienced security briefer or a graduate of the SBC; have a need to train others to prepare and present security briefings; and have a working knowledge of security requirements. If you want to learn *how* to brief—choose the SBC.

To host the courses described above, please call Linda Braxton or Gussie Scardina, DoDSI, at (804) 279-6076/5308 or DSN 695-6076/5308.

These courses are held in succession. The TTT precedes the SBC.

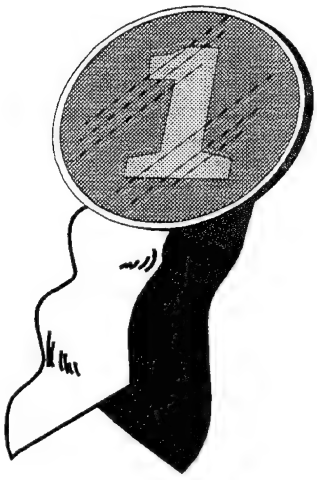
To host the SBC, you must be able to provide:

- ☐ one main classroom for 24 students
- ☐ 3 breakout rooms for 6 students each
- ☐ A-V equipment for all 4 rooms (Overhead projectors, screens, and writing surfaces for each room)
- ☐ At least two of the instructors and preferably more for the TTT.
- ☐ An on-site coordinator
- ☐ Invitations to other security organizations in your area in order to fill a class of 24.

The Department of Defense Security Institute (DoDSI) will:

- ✔ Provide the lead instructor and assume responsibility for the teaching success of the course.
- ✔ If necessary, provide security personnel from other organizations to help teach the course.
- ✔ Provide two full days of training for the instructors prior to starting the course.
- ✔ Provide the instructional materials in sufficient quantities for 24 students.
- ✔ Help the trainers teach the Security Briefers Course.

Attention Security Educators, here's your chance to sign up for the:



Security Briefers Course!

The Security Briefers Course will be offered at the
DoD Security Institute
in Richmond, Virginia, on these dates

Train-the-Trainer	**Security Briefers Course**
March 18-22, 1996	March 20-22, 1996
June 3-7, 1996	June 5-7, 1996
September 9-13, 1996	September 11-13, 1996

If interested in attending, or if you'd like to host this course,
call Linda Braxton at (804) 279-6076, DSN 695-6076.

In addition we are teaching on location at:

Holloman AFB, New Mexico
February 12-16, 1996
POC is Msgt. Kemp
(505) 475-1085, DSN 867-1085

Special Access Programs: Policy and Oversight

Policy Perspective

On January 5, 1994, the Deputy Secretary of Defense (DEPSECDEF) significantly enhanced changes in the DoD Special Access Program (SAP) management and control structures. This newsletter highlights those changes. The plan standardized and formalized the special access program approval, termination, revalidation and restructuring process through the Special Access Program Oversight Committee (SAPOC). A Senior Review Group (SRG) was established to support the SAP Oversight Committee principals. All special access programs are briefed to the SAP Oversight Committee, chaired by the Deputy Secretary of Defense, after being processed by the Senior Review Group and the appropriate central offices.

Special Access Program Policy

All special access programs (SAPs) will be reviewed and validated annually for continued SAP status by the OSD SAP Oversight Committee. The review takes a comprehensive look at cost, schedule, performance, and validates the need for continued compartmentation of restructuring to another SAP, a collateral program, or termination. The review also provides an avenue to ensue reciprocity and eliminates redundancy in similar programs. The Deputy Secretary of Defense is the final decision maker in establishing, disestablishing, or restructuring special access programs.

Special Access Program Oversight Committee Functions

The Special Access Program Oversight Committee (SAPOC) provides departmental oversight and management over all DoD special access programs; monitors programs to ensure compliance with law, regulations, policies and procedures; and ensures required information is provided to the Congress.

Special Access Program Oversight Committee Membership

The Special Access Program Oversight Committee is chaired by the Honorable John Deutch, Deputy Secretary of Defense, with permanent members from the Under Secretary of Defense (Acquisition & Technology), Under Secretary of Defense (Policy), Vice Chairman of the Joint Chiefs of Staff, and the Assistant Secretary of Defense (Command, Control, Communications, & Intelligence). The Office of Under Secretary of Defense (Acquisition & Technology) serves as both member and executive secretary to the SAP Coordinating Office (SAPCO). SAP Oversight Committee membership is not further delegable. Others may be invited by the Chairman when needed; such as the General Counsel, the Comptroller, the Assistant Secretary of Defense (Special Operations/Low Intensity Conflict), Assistant to the Secretary of Defense for Legislative Affairs, or the Director, Program Analysis & Evaluation.

The Senior Review Group

The Senior Review Group provides the principal support to the SAP Oversight Committee. It is composed of senior leadership (non-delegable) from Under Secretary of Defense for Policy, Under Secretary of Defense (Acquisition and Technology), Vice Chairman of the Joint Chiefs of Staff, and Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). The Deputy Director of the SAP Coordinating Office provides staff support. All special access programs are briefed to the Senior Review Group prior to presentation to the SAP Oversight Committee. Basically, the Senior Review Group is a "working level" group that reviews all special access programs prior to the SAP Oversight Committee briefing. Program managers provide detailed briefings to the Senior Review Group regarding potential questions or concerns that might be addressed during the SAP Oversight Committee.

The Special Access Program Coordinating Office

The SAP Coordinating Office director and deputy serve as the primary staff support to the SAP Oversight Committee. The SAP Coordinating Office serves as the primary point of contact with Congress, the National Security Council, and other government agencies.

Reprinted from SAPOC Information Bulletin, July 1994

DoD Security Institute
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, Virginia 23297-5091

Registration Request

Please print or type, and fill in all *applicable* information. In addition to serving as a permanent record of your registration, a class roster will be compiled prior to class from the information on this form. The roster will include your name, position, address, and phone number. If you have objections to this, please let us know. If you have any questions, call the Registrar (804) 279-4758/4892, DSN 695-4758/4892 (FAX 6406).

Privacy Act Statement

Authority: 5 USC 301 and DoD Directive 5105.42.

Principal Purpose or Purposes: The primary purpose served by DSI Form 2021A is to serve as a permanent enrollment record. Social security number (SSN) is required to distinguish between records of students with the same name.

Routine Uses: DSI Form 2021A is routinely used as an alphabetical index and locator card for students and as a course completion record.

Disclosure: Disclosure of information, including SSN, is voluntary. Failure to provide such information could result in inaccurate records of students with same name.

Course title	Course no.	Course dates

Social Security Number	Name (Last)	(First)	(MI)	(subtitle: Jr., III, etc.)

(Mr./Mrs../Ms.)	Rank/Rate	Position	Mil/GS Grade

Agency/Activity Code (see reverse for codes)	Birth date MM/DD/YY	Gender (circle) F M	Clearance level (circle) C S TS None

Duty station/Facility address	Job Title/Name/Address of Supervisor (if same address ☐)
(city) (state) (zip)	

DSN: _____ DSN: _____

Commercial No. _____ Commercial No. _____

Fax: _____ Fax: _____

E-mail address: _____ E-mail address: _____

Education level (see below)	Last college date MM/DD/YY	Years in security field	Years as adjudicator

Education level: High school, Some college, Associate, Bachelor, Masters, PhD., JD,

DoDSI supports the Americans with Disabilities Act of 1990. Attendees with special needs should indicate those needs here, or call (804) 279-4758/4892, DSN 695-4758/4892.

Attendance approved by official? (if identified in the course description sheet) Yes No

Agency/Activity Codes

Department of Defense

DAF	Air Force
DAY	Army
DAA	Defense Contract Audit Agency
DIO	Defense Information Services Organization
DSA	Defense Information Systems Agency
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DLA	Defense Logistics Agency
DMA	Defense Mapping Agency
DNA	Defense Nuclear Agency
DCR	Directorate for Industrial Security Clearance Review
DJS	Joint Chiefs of Staff
DJT	Joint Command
DMC	Marine Corps
DNS	National Security Agency
DNY	Navy
DSD	Secretary of Defense
DoD	Other Department of Defense

Other Government

AID	Agency for International Development
OAG	Agriculture Department
OCM	Commerce Department
OEB	Other Executive Branch
OED	Education Department
OEG	Energy Department
OEP	Environmental Protection Agency
OFE	Federal Emergency Management Agency
OFG	Foreign Government
OGA	General Accounting Office
OGS	General Services Administration
OHS	Health and Human Services Department
OIN	Interior Department
OIC	Intelligence Community
OJU	Justice Department
OLA	Labor Department
OLC	Library of Congress
ONA	National Aeronautics and Space Administration
OSF	National Science Foundation
OTO	North Atlantic Treaty Organization
ONR	Nuclear Regulatory Commission
OPM	Office of Personnel Management
OSB	Small Business Administration
OST	State Department
OTP	Transportation Department
OTR	Treasury Department
OAC	U.S. Arms Control and Disarmament Agency
OCP	U.S. Capitol Police
OIA	U.S. Information Agency
OPS	U.S. Postal Service
OSS	U.S. Senate/House of Representatives
OVA	Veterans Affairs Department
SPB	Security Policy Board

Private Industry

IND	Private Industry

The Security Awareness and Education Subcommittee proudly announces the release of a new video:

As Others See You

Understanding and Reporting Foreign Intelligence Threats

Designed with the scientist in mind — and those in the technical community who safeguard critical technologies, sensitive proprietary data, and government classified information. This video shows that the loss of this information can weaken our national security and dull our economic edge.

In this dramatization, we meet Dr. Woolrich, staff scientist from a U.S. Government laboratory, who is confronted by five foreign admirers, each in a different professional role. Any one of them, despite their credentials, could in reality be a foreign agent or an undercover source for a foreign intelligence service. Which one, if any, is the agent? The audience can learn an important lesson from this fictional scientist, especially if they later find themselves approached by a foreign representative.

Produced for the SAES by the Department of Energy's Office of Counterintelligence, with the assistance of Federal agencies represented on the subcommittee. Run time: 16 minutes. To obtain a 1/2-inch VHS copy, send a check or money order for $9.95 to:

CopyMaster Video Inc.
P.O. Box 684
Department 15
Villa Park, IL 60181

Allow 2-3 weeks for delivery.

For additional information, phone CopyMaster at (708) 279-1276.

Each copy of the video comes with an 18-page presenter's guide which describes specific objectives for awareness programs designed to prevent the loss of critical technology.

Attention !

Program Managers

System Security Engineers

Acquisition Systems Personnel

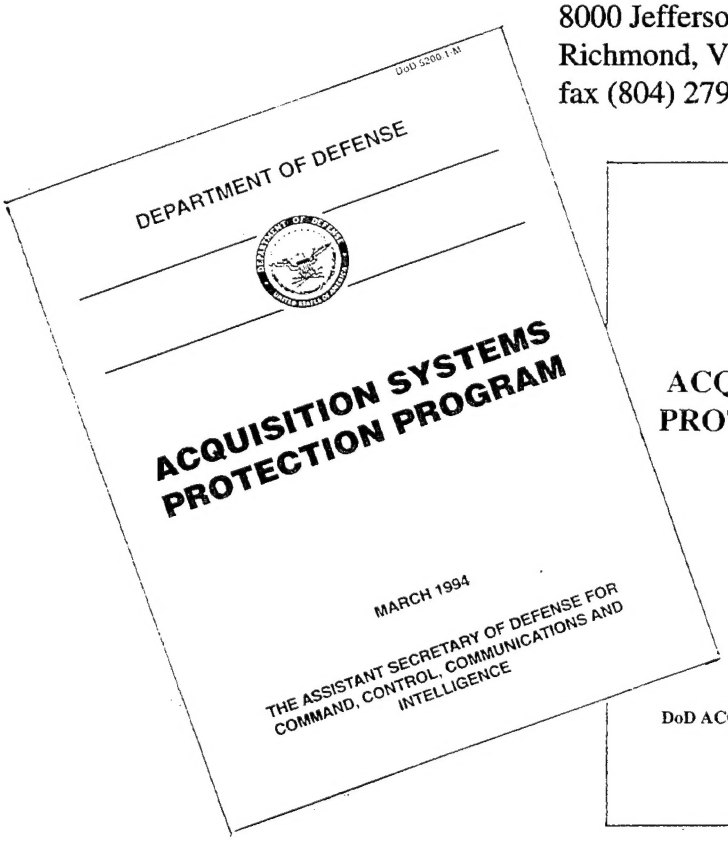
Yours for the asking:....

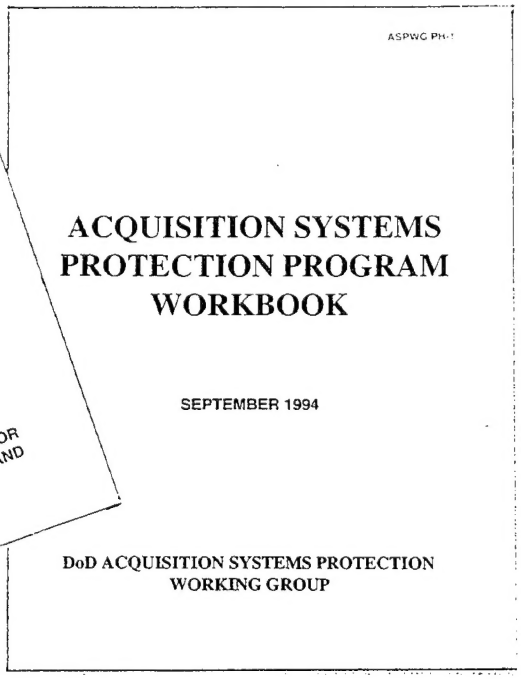
DOD 5200.1-M, Acquisition Systems Protection Program Manual

ASPWG PH-1, Acquisition Systems Protection Workbook

To help get your ASP program off the ground, DODSI will provide a copy of either or both of the above publications at your request. Send us a pre-addressed mailing label and a note stating how many copies of each your organization needs.

DOD Security Institute
ATTN: SEAT
8000 Jefferson Davis Hwy., Bldg 33E
Richmond, VA 23297-5091
fax (804) 279-6406, DSN 695-6406





New Awareness Video Available!

Protecting Critical Defense Information

A security video with a message for

Program Managers

Commanding Officers

Senior Executives

Executive Officers in Industry

and all who have administrative responsibility in the Department of Defense and Defense Industry

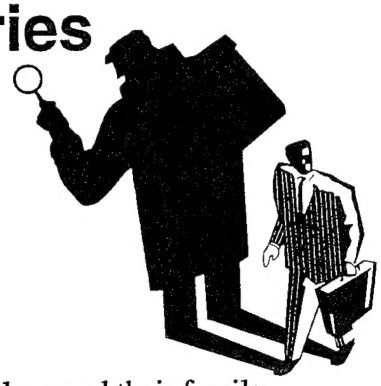
This 7-minute presentation, narrated by Adm. William O. Studeman, Deputy Director, Central Intelligence, has been developed especially for executives and managers in military organizations, government, and industry who have very limited time for briefings or training but who must be reminded of their continuing security responsibilities.

To obtain a copy for your firm or government security office, send a check for $9.95 to:

CopyMaster Video Inc.
P.O. Box 684
711 Fairfield
Villa Park, IL 60181
phone: (708) 279-1276

Department of Defense components and agencies, call (804) 279-3824, DSN 695-3824 to obtain a copy.

The Countering Espionage Series Video #2



It's Not a Victimless Crime

A 20-minute presentation, based on interviews of convicted espionage felons and their family members, designed to establish the fact that espionage has real victims; it is personally devastating not only to the offender but to those most closely associated with him.

This is the second in the Countering Espionage Series, each focusing on a different aspect of espionage and what can be learned from the point of view of the offender. This video is very similar to "You Can Make a Difference," the first in the series. A third video, "On Becoming a Spy" is due to be released in December and should be available from the same sources.

"It's Not a Victimless Crime" is marked For Official Use Only. It can not be make available for public viewing nor can it be released to the public media. Now being distributed to Federal agencies and departments, cleared government contractors may obtain a copy by written request to FilmComm.

To government contractors: Because this is an FOUO product, we ask that you certify in your order that when received, "This video product will be used only for the training and education of employees or personnel and in support of a federal government security program."

Prepaid cost is $21.50 plus $2.50 for shipping (1/2" VHS)(For 3/4" add $10.00) Invoiced requests are $23.50 and $2.50 for shipping.

For additional ordering details, call FilmComm.

Order from:

FilmComm Inc.
641 North Avenue
Glendale Heights, Il 60139
(708) 790-3300
fax: (708) 790-3325

This video has been produced by the Department of Defense Security Institute in cooperation with the Intelligence Community and Project Slammer.

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your address label

Our address is:

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314/4223 or DSN 695-5314/4223

- ❑ **Recent Espionage Cases: Summaries and Sources**. July 1994. Eighty-five cases, 1975 through 1994. "Thumb-nail" summaries and open-source citations.
- ❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee.
- ❑ **Terminator VIII**. Requirements for destruction of classified materials. Written specifically for the Department of Defense employee.
- ❑ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.
- ❑ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee.
- ❑ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment.
- ❑ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms.
- ❑ **Take A Security Break.** Questions and answers on security and other topics.
- ❑ **Take Another Security Break.** More questions and answers.
- ❑ **Lock Up!** A pamphlet on the structural standards and other security requirements for the storage of conventional arms, ammunition, and explosives.

Security Awareness Bulletin. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

- ❑ The Case of Randy Miles Jeffries **(2-90)**
- ❑ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)**
- ❑ Foreign Intelligence Threat for the 1990s **(4-90)**
- ❑ Regional Cooperation for Security Education **(1-91)**
- ❑ AIS Security **(2-91)**
- ❑ Economic Espionage **(1-92)**
- ❑ OPSEC **(3-92)**
- ❑ What is the Threat and the New Strategy? **(4-92)**
- ❑ Acquisition Systems Protection **(1-93)**
- ❑ Treaty Inspections and Security **(2-93)**
- ❑ Research on Espionage **(1-94)**
- ❑ Information Systems Security **(2-94)**
- ❑ Acquisition Systems Protection Program **(3-94)**
- ❑ Aldrich H. Ames Espionage Case **(4-94)**
- ❑ Revised Self-Inspection Handbook/Summary of NISPOM Changes **(1-95)**
- ❑ The Threat to U.S. Technology **(2-95)**